STATEWIDE INFORMATION SYSTEMS STANDARD

Statewide Standard: Computer Security Incident Management

Effective Date: September 1, 2010

Approved: State of Montana Chief Information Officer

I. Purpose

The purpose of this **Computer Security Incident Management Standard** (Standard) is to establish the specifications and process requirements to implement the **Statewide Policy: Computer Security Incident Management** (Policy) for computer and information systems security.

II. Applicability

This Standard is applicable to parties subject to the **Statewide Policy: Computer Security Incident Management**.

III. Scope

This Standard specifies and requires the implementation of a computer security incident response controls plan, and associated procedures, for the information systems and assets managed or controlled by each agency.

This Standard encompasses computer security incident management of information systems (IS) for which agencies have administrative or statutory responsibility, including systems managed or hosted by third-parties on behalf of those agencies. It addresses incidents which may occur in the normal course of business activities of the agencies.

This Standard may conflict with other information system policies currently in effect. Where conflicts exist, the more restrictive instrument governs. The development of future policies or standards will explicitly identify and retire any superseded portions of current policies or standards.

IV. Definitions

For the purpose of this instrument, the phrase "incident response" shall be synonymous with "incident management."

Agency — Any entity of the executive branch, including the university system. Reference §2-17-506(8), MCA.

Information Security — The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability. Reference 44 U.S.C., Sec. 3542.

Information System	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. Reference 44 U.S.C. Sec. 3502.
Information Resources	Information and related resources, such as personnel, equipment, funds, and information technology. Reference 44 U.S.C. Sec. 3502.
Information Technology	Hardware, software, and associated services and infrastructure used to store or transmit information in any form, including voice, video, and electronic data. Reference §2-17-506(7), MCA.

Refer to the National Institute of Standards and Technology SP800-61 Revision 1 Computer Incident Handling Guide (NIST SP800-61), Appendix D - Glossary for a list of incident management-specific definitions.

Refer to the Statewide Information system Policies and Standards Glossary for a list of local definitions.

Refer to the National Information Assurance (IA) Glossary, at http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf for common information systems security-related definitions.

V. Requirements and Specifications

In compliance with the **Statewide Policy: Computer Security Incident Management**, the requirements and specifications for this Standardare listed below:

A. Management Requirements

Each agency shall ensure that an organization structure is in place to:

1. Implement this Standard through procedure(s);
2. Assign information system security responsibilities;
3. Respond to security incidents;
4. Develop process(es) and procedure(s) to measure compliance with this Standard.

Agency Heads	The agency head (or equivalent present executive officer) has overall responsibility for providing adequate resources to support the information system security incident management program.
Agency Personnel	Agency personnel are responsible for reporting real or suspected IS security incidents as specified by their procedure(s).

Information Security Officer

The Information Security Officer (also known as the Information Systems Security Officer) may be the same individual designated by the agency head to administer the agency's security program for data under §MCA 2-15-114. Security Responsibilities Of Departments For Data. Specific responsibilities under this Standard are:

1. Evaluating real or suspected IS security incidents within the agency and all component organizations;

2. Providing resolution recommendations to the agency head, any attached agencies and division administrators; and

3. Developing agency policies, standards, and procedures in evaluating and referring the investigation to other qualified entities, including law enforcement.

B. Performance Requirements

Each agency shall develop and implement an ***incident management program,*** establishing ***general requirements*** within an Incident Management Standard(s) that:

1. Specifies general controls based on NIST SP800-61 Revision 1

2. Specifies levels of Incident Management Standard(s) and controls based upon the following requirements:

    a. As determined by completion of the risk management process based upon NIST SP800-39 Managing Risk from Information Systems – An Organizational Perspective. After review of the risk assessment(s), agency management shall determine any changes in the level of process, standards and controls.

    Or…

    b. Implement the **lowest** level of incident response standards and controls based upon NIST SP800-53 Recommended Security Controls for Federal Information Systems (latest revision), Annex 1, Low-Impact Baseline incident response (IR) family (known as **Annex 1**) not later than **September 1, 2010**.

3. Implements this Incident Management Standard through procedure(s).

4. Allocates adequate resources to respond quickly and effectively when information systems are breached.

5. Invokes their Incident Management procedure(s) for each declared incident.

6. Reviews the Incident Management program, process and procedure(s) annually, and implement authorized changes to policy, standard(s), or procedure(s).

7. Integrates Incident Management plans, standards and procedures with operational and information requirements of the common and central incident management function provided by the Department of Administration.

VI. Compliance

Compliance with this Standard shall be evidenced by adherence to the compliance criteria listed in Annex A - Compliance Criteria - Computer Security Incident Management (attached). Note: "Annex A" is not to be confused with NIST SP 800-53 Annexes 1, 2, and 3.

VII. Change Control and Exceptions

Standard changes or exceptions are governed by the Procedure for Establishing and Implementing Statewide Information Technology Policies and Standards. Requests for a review or change to this instrument are made by submitting an Action Request form (at http://itsd.mt.govcontent/content/policy/policies/action_request.doc). Requests for exceptions are made by submitting an Exception Request form (at http://itsd.mt.gov/content/policy/policies/exception_request.doc). Changes to policies and standards will be prioritized and acted upon based on impact and need.

VIII. Closing

For questions or comments about this instrument, contact the State of Montana Chief Information Officer at ITSD Service Desk (at http://servicedesk.mt.gov/ess.do), or:

PO Box 200113
Helena, MT 59620-0113
(406) 444-2700
FAX: (406) 444-2701

IX. Cross-Reference Guide

A. Federal/State Laws

- §2-15-114 MCA – Security Responsibilities of Departments for Data.
- §2-17-534 MCA - Security Responsibilities of Department.

B. State Policies (IT Policies, MOM Policies, ARM Policies)

- MOM 3-0130 Discipline

C. IT Procedures or Guidelines

- Guide To NIST Information Security Documents

- NIST SP800-61 Revision 1 Computer Incident Handling Guide
- NIST SP800-53 Revision 2 Recommended Security Controls for Federal Information Systems
- NIST SP800-53 Recommended Security Controls for Federal Information Systems (latest revision), Annex 1, Low-Impact Baseline incident response (IR) family
- NIST SP800-53 Recommended Security Controls for Federal Information Systems (latest revision), Annex 2, Moderate-Impact Baseline incident response (IR) family
- NIST SP800-53 Recommended Security Controls for Federal Information Systems (latest revision), Annex 3, High-Impact Baseline incident response (IR) family
- NIST SP800-84 Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities
- FIPS PUB 199 - Standards for Security Categorization of Federal Information and Information Systems
- Statewide Policy: Establishing and Implementing Statewide Information Technology Policies and Standards
- Statewide Procedure: Establishing and Implementing Statewide Information Technology Policies and Standards

X. Administrative Use

Product ID:	STND-20081029a
Proponent:	Chief Information Officer
Version:	1.0.3
Version Date:	2/17/2009
Approved Date:	February 17, 2009
Effective Date:	September 1, 2010
Change & Review Contact:	ITSD Service Desk (at http://servicedesk.mt.gov/ess.do)
Review:	Event Review: Any event affecting this architecture paper may initiate a review. Such events may include a change in statute, key staff changes or a request for review or change.
Scheduled Review Date:	September 1, 2015
Last Review/Revision:	
Changes:	